Australian Government
Australian Cyber Security Centre

ACSC
AUSTRALIAN CYBER SECURITY CENTRE

PROTECT

July 2015

Hardening Microsoft Windows 8.1 Standard Operating Environments

Workstations are often targeted by an adversary using malicious webpages, emails with malicious attachments and removable media with malicious content in an attempt to extract sensitive information. Hardening the operating environments of workstations is an important part of reducing this risk.

This document provides guidance on assessing Microsoft Windows operating environments for vulnerabilities, or lack of security controls, that would potentially allow an adversary to compromise a workstation and extract sensitive information. This document does not cover supplementary security controls that should be applied to an organisation's environment such as physical, personnel and network security controls. While this document refers to workstations, most group policy recommendations are equally applicable to servers using Microsoft Server 2012 R2. In cases where group policies are not applicable to servers, specific server group policies have been included for completeness. The names and locations of group policies used in this document are taken from Microsoft Windows 8.1; some slight differences may exist for earlier versions of Microsoft Windows. Before implementing recommendations in this document, thorough testing should be undertaken to ensure the potential for unintended negative impacts on business processes is reduced as much as possible.

This document is intended for information technology and information security professionals within organisations looking to undertake risk assessments or vulnerability assessments as well as those wishing to develop a hardened standard operating environment for workstations.

High Severity Issues

An issue of high severity indicates a vulnerability which may allow a workstation to be compromised by an adversary resulting in immediate access to privileged accounts, resources or sensitive information. Alternatively, a high severity issue discusses the lack of security controls which would mitigate common intrusion techniques.

Standard Operating Environment

When users are left to setup, configure and maintain their own workstations it can very easily lead to an inconsistent and insecure environment where particular workstations are more vulnerable than others. This inconsistent and insecure environment can easily allow an adversary to gain an initial foothold on a network. To reduce this risk, workstations should connect to a domain using a standard operating environment that is centrally controlled and configured by experienced information technology and information security professionals.

Application Whitelisting

An adversary can email malicious code, or host malicious code on a compromised website, and use social engineering techniques to convince users into executing it on their workstation. Such malicious code often aims to exploit vulnerabilities in existing applications and doesn't need to be installed on the workstation to be successful. To reduce this risk, an application whitelisting solution should be appropriately implemented. Application whitelisting when implemented in its most effective form (e.g. using hashes for executables, dynamic link libraries, scripts, installers and packaged apps) can be an extremely effective mechanism in not only preventing malicious code from executing but also ensuring only authorised applications can be installed on workstations. Less effective implementations of application whitelisting (e.g. using approved paths for installed applications in combination with access controls requiring privileged access to write to these locations) can be used as a first step towards implementing a more comprehensive application whitelisting solution.

For more information on application whitelisting and how it can be appropriately implemented see *Application Whitelisting Explained*[1] and '*Top 4' Strategies to Mitigate Targeted Cyber Intrusions: Mandatory Requirement Explained*[2].

If Microsoft AppLocker[3] is used for application whitelisting, the following rules can be used as a sample path-based implementation. In support of this, the rules, enforcement of rules and the automatic starting of the Application Identity service should be set via group policy at a domain level. Furthermore, both 16-bit legacy application and POSIX subsystem support should be disabled[4].

Whitelisting Rule	Recommended Value
Computer Configuration\Policies\Windows Settings\Security Settings\Application Control Policies\AppLocker\DLL Rules	
[Path] (Default Rule) All DLLs	Allow BUILTIN\Administrators
[Path] (Default Rule) All DLLs located in the Program Files folder	Allow Everyone

Whitelisting Rule	Recommended Value
[Path] (Default Rule) Microsoft Windows DLLs	Allow Everyone Exceptions: %SYSTEM32%\Microsoft\Crypto\RSA\MachineKeys* %SYSTEM32%\spool\drivers\color* %SYSTEM32%\Tasks* %WINDIR%\debug\WIA* %WINDIR%\Tasks* %WINDIR%\Temp*
Computer Configuration\Policies\Windows Settings\Security Settings\Application Control Policies\AppLocker\Executable Rules	
[Path] (Default Rule) All files	Allow BUILTIN\Administrators
[Path] (Default Rule) All files located in the Program Files folder	Allow Everyone
[Path] (Default Rule) All files located in the Windows folder	Allow Everyone Exceptions: %SYSTEM32%\Microsoft\Crypto\RSA\MachineKeys* %SYSTEM32%\spool\drivers\color* %SYSTEM32%\Tasks* %WINDIR%\debug\WIA* %WINDIR%\Tasks* %WINDIR%\Temp*
Computer Configuration\Policies\Windows Settings\Security Settings\Application Control Policies\AppLocker\Packaged app Rules	
[Publisher] Microsoft Corporation	Allow Everyone
Computer Configuration\Policies\Windows Settings\Security Settings\Application Control Policies\AppLocker\Script Rules	
[Path] (Default Rule) All scripts	Allow BUILTIN\Administrators
[Path] (Default Rule) All scripts located in the Program Files folder	Allow Everyone

Whitelisting Rule	Recommended Value
[Path] (Default Rule) All scripts located in the Windows folder	Allow Everyone Exceptions: %SYSTEM32%\Microsoft\Crypto\RSA\MachineKeys* %SYSTEM32%\spool\drivers\color* %SYSTEM32%\Tasks* %WINDIR%\debug\WIA* %WINDIR%\Tasks* %WINDIR%\Temp*
Computer Configuration\Policies\Windows Settings\Security Settings\Application Control Policies\AppLocker\Windows Installer Rules	
[Publisher] (Default Rule) All Windows Installer files	Allow BUILTIN\Administrators

Application Versions and Security Patches

While some vendors may release new application versions to address vulnerabilities, others may release security patches. If new application versions and security patches for applications are not installed it can allow an adversary to easily compromise workstations. This is especially important for key applications that interact with content from untrusted sources such as office productivity suites (e.g. Microsoft Office), PDF readers (e.g. Adobe Reader), web browsers (e.g. Microsoft Internet Explorer, Mozilla Firefox or Google Chrome), common web browser plugins (e.g. Adobe Flash), email clients (Microsoft Outlook) and software platforms (e.g. Oracle Java Platform and Microsoft .Net Framework). To reduce this risk, new application versions and security patches for applications should be applied in an appropriate timeframe as determined by the severity of vulnerabilities they address and any mitigating measures already in place. In cases where a previous version of an application continues to receive support in the form of security patches it still should be upgraded to the latest version to receive the benefit of any new security functionality; however, this may be done as soon as practical rather than within two days of release.

For more information on determining the severity of vulnerabilities and timeframes for applying new application versions and security patches for applications see *Assessing Security Vulnerabilities and Patches*[5].

Operating System Patching

Security patches are released either in response to previously disclosed vulnerabilities or to proactively address vulnerabilities that have not yet been publicly disclosed. In the case of disclosed vulnerabilities, it is possible that exploits have already been developed and are freely available in common hacking tools. In the case of security patches for vulnerabilities that have not yet been publically disclosed, it is relatively easy for an adversary to use freely available tools to identify the vulnerability being patched and develop an associated exploit. This activity can be undertaken in less than one day and has led to an increase in 1-day attacks. To reduce this risk, operating system security patches and driver updates should be centrally managed and deployed in an appropriate timeframe as determined by the severity of the vulnerability and any mitigating measures already in

place. This can be achieved using Microsoft System Center Configuration Manager (SCCM)[6]. Microsoft Windows Server Update Services (WSUS)[7] can also centrally deploy security patches but only for Microsoft applications.

For more information on determining the severity of vulnerabilities and timeframes for applying security patches see *Assessing Security Vulnerabilities and Patches*[8].

The following group policies can be implemented to ensure operating systems remain appropriately patched.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\Printers	
Extend Point and Print connection to search Windows Update	Disabled
Computer Configuration\Policies\Administrative Templates\System\Device Installation	
Specify search order for device driver source locations	Enabled Select search order: Do not search Windows Update
Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings	
Turn off access to all Windows Update features	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Installer	
Allow users to patch elevated products	Disabled
Prevent users from using Windows Installer to install updates and upgrades	Disabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update	
Allow Automatic Updates immediate installation	Enabled
Allow non-administrators to receive update notifications	Enabled
Allow signed updates from an intranet Microsoft update service location	Enabled
Automatic Updates detection frequency	Enabled Check for updates at the following interval (hours): 22

Group Policy	Recommended Value
Configure Automatic Updates	Enabled Configure automatic updating: 4 - Auto download and schedule the install Schedule install day: 0 – Every day Schedule install time: 03:00
Do not connect to any Windows Update Internet locations	Enabled
Enable client-side targeting	Enabled Target group name for this computer: *<as required>*
No auto-restart with logged on users for scheduled automatic updates installations	Disabled
Specify intranet Microsoft update service location	Enabled Set the intranet update service for detecting updates: *<server:port>* Set the intranet statistics server: *<server:port>*
Turn on recommended updates via Automatic Updates	Enabled

Alternatively, if a Windows Server Update Services (WSUS)[9] server is not used, the following group policies can be implemented to access Microsoft Windows updates over the Internet.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\System\Device Installation	
Specify search order for device driver source locations	Enabled Select search order: Search Windows Update First
Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings	
Turn off access to all Windows Update features	Disabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update	
Do not connect to any Windows Update Internet locations	Disabled
Enable client-side targeting	Disabled

Group Policy	Recommended Value
Specify intranet Microsoft update service location	Disabled

Privileged Accounts

Providing users with a privileged account for day to day usage poses a risk that they will use this account for external web and email access. This is of particular concern as privileged users have the ability to execute malicious code with privileged access rather than standard access. To reduce this risk, users that don't require privileged access should not be granted privileged accounts while users that require privileged access should have separate standard and privileged accounts with different credentials. In addition, any privileged accounts used should have external web and email access blocked.

For more information on the use of privileged accounts and minimising their usage see *Restricting administrative privileges explained*[10] and '*Top 4' Strategies to Mitigate Targeted Cyber Intrusions: Mandatory Requirement Explained*[11].

Application Hardening

When applications are installed they are often not pre-configured in a secure state. By default, many applications enable functionality that isn't required by any users while in-built security functionality may be disabled or set at a lower security level. For example, Microsoft Office by default allows untrusted macros in Office documents to automatically execute without user interaction. To reduce this risk, applications should have any in-built security functionality enabled and appropriately configured along with unrequired functionality disabled. This is especially important for key applications such as office productivity suites (e.g. Microsoft Office), PDF readers (e.g. Adobe Reader), web browsers (e.g. Microsoft Internet Explorer, Mozilla Firefox or Google Chrome), common web browser plugins (e.g. Adobe Flash), email clients (Microsoft Outlook) and software platforms (e.g. Oracle Java Platform and Microsoft .Net Framework). In addition, vendors may provide guidance on configuring their products securely. For example, Microsoft provides the *Microsoft Office 2010 SP1 Security Guide* as part of the Microsoft Security Compliance Manager tool[12]. In such cases, vendor guidance should be followed to assist in securely configuring their products.

Operating System Architecture

The x64 (64-bit) versions of Microsoft Windows include additional security functionality that the x86 (32-bit) versions lack. This includes native hardware-based Data Execution Prevention (DEP) kernel support, Kernel Patch Protection (PatchGuard), mandatory device driver signing and lack of support for malicious 32-bit drivers or 16-bit code. Using x86 (32-bit) versions of Microsoft Windows exposes organisations to exploit techniques mitigated by x64 (64-bit) versions of Microsoft Windows. To reduce this risk, workstations should use the x64 (64-bit) versions of Microsoft Windows.

Enhanced Mitigation Experience Toolkit

An adversary that develops exploits for Microsoft Windows will have a higher success rate when measures designed by Microsoft to help prevent vulnerabilities from being exploited are not appropriately implemented. The Enhanced Mitigation Experience Toolkit (EMET)[13] was designed by the Microsoft Security Research Center (MSRC) engineering team to provide a number of system wide mitigation measures such as DEP, ASLR, SEHOP and SSL/TLS certificate trust pinning, while also providing additional application specific mitigation measures. Mitigation measures that can be defined on an application by application basis include: null page pre-allocation, common heap spray address pre-allocation, export address table access filtering, bottom-up virtual memory randomization, checking and preventing LoadLibary calls against UNC paths, special checking on memory protection

APIs, ROP mitigation for critical functions, simulating execution flows, and checking if a stack pointer was pivoted. To reduce the risk of an adversary easily creating exploits for Microsoft Windows, the latest version of EMET should be appropriately implemented.

The group policies for EMET are provided in the EMET installation directory. The ADMX and associated en-us ADML file for EMET can be placed in *C:\Windows\SYSVOL\domain\Policies\PolicyDefinitions* on the Domain Controller and they will automatically be loaded in the Group Policy Management Editor. Of note, each time changes are made to EMET group policies on the Domain Controller, the *emet_conf --refresh* command will need to be run via a script or scheduled task on workstations to import the changes to the EMET configuration.

The following group policies can be implemented to ensure EMET is appropriately implemented.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\Windows Components\EMET	
Application Configuration	Enabled <*organisation defined*>
Default Action and Mitigation Settings	Enabled Deep Hooks: Enabled Anti Detours: Enabled Banned Functions: Enabled Exploit Action: Stop Program
Default Protections for Internet Explorer	Enabled
Default Protections for Popular Software	Enabled
Default Protections for Recommended Software	Enabled
EMET Agent Custom Message	Enabled Tray Icon Message: <*organisation defined*>
EMET Agent Visibility	Enabled Start Agent Hidden: Disabled
Reporting	Enabled Event Log: Enabled Tray Icon: Enabled Early Warning: Disabled
System ASLR	Enabled ASLR Setting: Application Opt-In

Group Policy	Recommended Value
System DEP	Enabled DEP Setting: Always On
System SEHOP	Enabled SEHOP Setting: Application Opt-Out

Data Execution Prevention

Data Execution Prevention (DEP) is a security function that can help protect workstations by monitoring applications to ensure they use memory safely. If DEP notices an application attempting to execute instructions from a portion of memory used for data it will close the application and notify the user. The default setting for desktop lines of Microsoft Windows is *Turn on DEP for essential Windows programs and services only*. This default setting does not cover non-Windows programs and will fail to block malicious code that would otherwise be blocked if DEP was applied to it. To reduce this risk, DEP, preferably hardware-based, should be enabled for all applications and services except those that need to be explicitly excluded for compatibility reasons. To enable DEP for all applications and services, except those that need to be explicitly excluded, the DEP setting within Microsoft Windows can be changed to *Turn on DEP for all programs and services except those I select*. This can be set under the Data Execution Prevention tab within the Performance Options of System Properties. Additionally, if the CPU supports hardware-based DEP, the text *Your computer's processor supports hardware-based DEP* will be displayed. Should there be a need to force the use of DEP for all applications and services, the Enhanced Mitigation Experience Toolkit[14] from Microsoft can be used to set DEP to *Always On*. This toolkit can also be used to determine the DEP status of running processes at any given time. The Process Explorer tool[15] in the Windows Sysinternals suite[16] can also display this information.

The following group policy can be implemented to ensure DEP is used in File Explorer.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer	
Turn off Data Execution Prevention for Explorer	Disabled

Address Space Layout Randomization

An adversary may attempt to compromise a workstation by accessing the location of important information in memory such as an executable's base address and the position of the heap, stack and libraries in a process' address space. To reduce this risk, Address Space Layout Randomization (ASLR) should be enabled for all applications that support it. By default, ASLR is enabled from Microsoft Windows Vista onwards and can mitigate some forms of attacks by randomising the location of important information in memory. The use of ASLR can be confirmed by using the Enhanced Mitigation Experience Toolkit from Microsoft[17] to ensure ASLR is set to *Application Opt In*.

Structured Exception Handling Overwrite Protection

Without Structured Exception Handling Overwrite Protection (SEHOP) an adversary can use Structured Exception Handler overwrite techniques to execute malicious code on a workstation. By default, SEHOP is disabled in the desktop line of Microsoft Windows. To reduce this risk, SEHOP should be enabled for all applications.

SEHOP can be enabled by using the Enhanced Mitigation Experience Toolkit from Microsoft[18] to set SEHOP to *Always On* or by implementing the following registry entry.

Registry Entry	Recommended Value
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Kernel	
DisableExceptionChainValidation	REG_DWORD 0x00000000 (0)

Secure Boot

Another method for malicious code to maintain persistence and prevent detection is to replace the default boot loader for Microsoft Windows with a malicious version. In such cases the malicious boot loader executes at boot time and loads Microsoft Windows without any indication that it is present. Such malicious boot loaders are extremely difficult to detect and can be used to conceal malicious code on workstations. To reduce this risk, motherboards with Secure Boot functionality should be used. Secure Boot, a component of Trusted Boot, is a new security feature supported by Microsoft Windows 8 and motherboards with an Unified Extensible Firmware Interface (UEFI). Secure Boot works by checking at boot time that the boot loader is signed and matches a Microsoft signed certificate stored in the UEFI. If the certificate signatures match the boot loader is allowed to run, otherwise it is prevented from running and the workstation will not boot.

Early Launch Antimalware

Another key security feature of Trusted Boot supported by Microsoft Windows 8 and motherboards with an UEFI is Early Launch Antimalware (ELAM) support. Used in conjunction with Secure Boot, an ELAM driver can be registered as the first non-Microsoft driver that will be initialised on a workstation as part of the boot process, thus allowing it to verify all subsequent drivers before they are initialised. The ELAM driver is capable of allowing only known good drivers to initialise; known good and unknown drivers to initialise; known good, unknown and bad but critical drivers to initialise; or all drivers to initialise. To reduce the risk of malicious drivers, only known good drivers should be allowed to be initialised during the boot process.

The following group policy can be implemented to ensure only known good drivers will be initialised at boot time.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\System\Early Launch Antimalware	
Boot-Start Driver Initialization Policy	Enabled Choose the boot-start drivers that can be initialized: Good and unknown

Measured Boot

The third key security feature of Trusted Boot supported by Microsoft Windows 8 and motherboards with both an UEFI and a Trusted Processing Module (TPM) is Measured Boot. Measured Boot is used to develop a reliable log of components that are initialised before the ELAM driver. This information can then be scrutinised by antimalware software for signs of tampering of boot components. To

reduce the risk that malicious changes to boot components go unnoticed, Measured Boot should be used on workstations that support it.

Host-based Intrusion Prevention

Many endpoint security applications rely on signatures to detect malicious code. This approach is only effective when a particular piece of malicious code has already been profiled and signatures are current. An adversary can create variants of known malicious code, or develop new unseen malicious code, to bypass traditional signature-based detection mechanisms. To reduce this risk, endpoint security applications with host-based intrusion prevention functionality (using heuristics to identify and block malicious behaviour) should be appropriately implemented. In doing so, heuristic functionality should be set at the highest level available.

Built-in Administrator Accounts

When built-in administrator accounts are used with common account names and passwords it can allow an adversary that compromises these credentials on one workstation to easily transfer across the network to other workstations. Even if built-in administrator accounts are uniquely named and have unique passwords, an adversary can still identify these accounts based on their security identifier (i.e. S-1-5-21-*domain*-500[19]) and use this information to focus any attempts to brute force credentials on a workstation if they can get access to the Security Accounts Manager (SAM) database. To reduce this risk, built-in administrator accounts should be disabled. Instead, domain accounts with local administrative privileges, but without domain administrative privileges, should be used for workstation management. Ideally, domain accounts unique to each workstation, and with unique passwords, should be used.

The following group policies can be implemented to disable and rename built-in administrator accounts.

Group Policy	Recommended Value
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Accounts: Administrator account status	Disabled

Multi-factor Authentication

As privileged credentials often allows users to bypass security functionality put in place to protect workstations, and are susceptible to key logging applications, it is important that they are appropriately protected against compromise. In addition, an adversary that brute forces captured password hashes can gain access to workstations if multi-factor authentication hasn't been implemented. To reduce this risk, hardware-based multi-factor authentication should be used for privileged users and considered for all other users.

For more information on how to effectively implement multi-factor authentication see *Multi-factor Authentication*[20].

When smart cards are used for multi-factor authentication, the following group policies can be implemented to control their use.

Group Policy	Recommended Value
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Interactive logon: Require smart card	Enabled

Group Policy	Recommended Value
Interactive logon: Smart card removal behavior	Lock Workstation

Software-based Firewalls

Network firewalls often fail to prevent the propagation of malicious code on a network, or an adversary from extracting sensitive information, as they generally only control which ports or protocols can be used between segments on a network. Many forms of malicious code are designed specifically to take advantage of this by using common protocols such as HTTP, HTTPS, SMTP and DNS. To reduce this risk, software-based firewalls that filter both incoming and outgoing traffic should be appropriately implemented. Software-based firewalls are more effective than network firewalls as they can control which applications and services can communicate to and from workstations. The in-built Windows firewall (from Microsoft Windows 7 onwards) can be used to control both inbound and outbound traffic for specific applications.

Virtualised Web and Email Access

An adversary can often deliver malicious code directly to workstations via external web and email access. Once a workstation has been exploited, an adversary can use these same communication paths for bi-directional communications to control their malicious code. To reduce this risk, web and email access on workstations should occur through a non-persistent virtual environment (i.e. using virtual desktops or virtual applications). When using a virtual environment, workstations will receive additional protection against intrusion attempts targeted at exploiting vulnerabilities in web browsers and email clients as any attempts, if successful, will execute in a non-persistent virtual environment rather than on a local workstation.

Audit Event Management

Failure to capture and analyse security related audit events from workstations can result in intrusions going unnoticed. In addition, the lack of such information can significantly hamper investigations following a security incident. To reduce this risk, security related audit events from workstations should be captured and routinely analysed.

The following group policies can be implemented to ensure security related audit events are appropriately captured.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Application	
Back up log automatically when full	Enabled
Control Event Log behavior when the log file reaches its maximum size	Enabled
Specify the maximum log file size (KB)	Enabled Maximum Log Size (KB): 20480
Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Security	
Back up log automatically when full	Enabled

Group Policy	Recommended Value
Control Event Log behavior when the log file reaches its maximum size	Enabled
Specify the maximum log file size (KB)	Enabled Maximum Log Size (KB): 20480
Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Setup	
Back up log automatically when full	Enabled
Control Event Log behavior when the log file reaches its maximum size	Enabled
Specify the maximum log file size (KB)	Enabled Maximum Log Size (KB): 20480
Turn on logging	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\System	
Back up log automatically when full	Enabled
Control Event Log behavior when the log file reaches its maximum size	Enabled
Specify the maximum log file size (KB)	Enabled Maximum Log Size (KB): 20480
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Error Reporting	
Disable logging	Disabled
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled
Audit: Shut down system immediately if unable to log security audits	Disabled
MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning	90%
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment	
Generate security audits	LOCAL SERVICE NETWORK SERVICE
Manage auditing and security log	Administrators

If fine grained control of event auditing is not required, coarse audit policies should be configured.

The following group policies can be implemented to enable a coarse event auditing strategy.

Group Policy	Recommended Value
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy	
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	No auditing
Audit logon events	Success, Failure
Audit object access	No auditing
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit process tracking	No auditing
Audit system events	Success, Failure
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	Disabled

If fine grained control of event auditing is required, advanced audit policies should be configured.

The following group policies can be implemented to enable a comprehensive event auditing strategy.

Group Policy	Recommended Value
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon	
Audit Credential Validation	Success and Failure
Audit Kerberos Authentication Service	No Auditing
Audit Kerberos Service Ticket Operations	No Auditing
Audit Other Account Logon Events	No Auditing
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management	
Audit Application Group Management	No Auditing
Audit Computer Account Management	Success and Failure
Audit Distribution Group Management	No Auditing
Audit Other Account Management Events	Success and Failure
Audit Security Group Management	Success and Failure

Group Policy	Recommended Value
Audit User Account Management	Success and Failure
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking	
Audit DPAPI Activity	No Auditing
Audit Process Creation	Success
Audit Process Termination	No Auditing
Audit RPC Events	No Auditing
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\DS Access	
Audit Detailed Directory Service Replication	No Auditing
Audit Directory Service Access	No Auditing
Audit Directory Service Changes	No Auditing
Audit Directory Service Replication	No Auditing
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Global Object Access Auditing	
File system	Not configured
Registry	Not configured
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff	
Audit Account Lockout	No Auditing
Audit IPSec Extended Mode	No Auditing
Audit IPSec Main Mode	No Auditing
Audit IPSec Quick Mode	No Auditing
Audit Logoff	Success
Audit Logon	Success and Failure
Audit Network Policy Server	No Auditing
Audit Other Logon/Logoff Events	No Auditing
Audit Special Logon	Success
Audit User / Device Claims	No Auditing
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access	

Group Policy	Recommended Value
Audit Application Generated	No Auditing
Audit Central Access Policy Staging	No Auditing
Audit Certification Services	No Auditing
Audit Detailed File Share	No Auditing
Audit File Share	No Auditing
Audit File System	No Auditing
Audit Filtering Platform Connection	No Auditing
Audit Filtering Platform Packet Drop	No Auditing
Audit Handle Manipulation	No Auditing
Audit Kernel Object	No Auditing
Audit Other Object Access Events	No Auditing
Audit Registry	No Auditing
Audit Removable Storage	No Auditing
Audit SAM	No Auditing
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change	
Audit Audit Policy Change	Success and Failure
Audit Authentication Policy Change	Success
Audit Authorization Policy Change	No Auditing
Audit Filtering Platform Policy Change	No Auditing
Audit MPSSVC Rule-Level Policy Change	No Auditing
Audit Other Policy Change Events	No Auditing
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Privilege Use	
Audit Non Sensitive Privilege Use	Success and Failure
Audit Other Privilege Use Events	No Auditing
Audit Sensitive Privilege Use	Success and Failure
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System	
Audit IPsec Driver	Success and Failure
Audit Other System Events	No Auditing

Group Policy	Recommended Value
Audit Security State Change	Success and Failure
Audit Security System Extension	Success and Failure
Audit System Integrity	Success and Failure
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	Enabled

Centralised Audit Event Logging

Storing audit event logs on workstations poses a risk that an adversary could attempt to modify or delete these logs during an intrusion to cover their tracks. In addition, failure to conduct centralised audit event logging will reduce the visibility of audit events across all workstations, prevent the correlation of audit events and increase the complexity of any investigations after security incidents. To reduce this risk, audit event logs from workstations should be transferred to a secure central logging server.

Medium Severity Issues

An issue of medium severity indicates a vulnerability which may allow a workstation to be compromised by an adversary but not result in immediate access to privileged accounts, resources or sensitive information. Alternatively, a medium severity issue discusses hardening countermeasures which can limit the severity of a compromise or help identify an adversary and the method used to gain access.

Operating System Functionality

Leaving unneeded functionality in Microsoft Windows enabled can provide greater opportunities for potentially vulnerable or misconfigured functionality to be exploited by an adversary. To reduce this risk, unneeded functionality in Microsoft Windows should be disabled or removed.

The following group policies can be implemented to disable the Windows Mail and Windows Messenger functionality while other commonly installed yet unneeded functionality (e.g. Media Features, Print and Document Services, Windows Location Platform, XPS Services and XPS Viewer) can be removed via the *Turn Windows features on or off* functionality within the Microsoft Windows Control Panel.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Mail	
Turn off Windows Mail application	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Messenger	
Do not allow Windows Messenger to be run	Enabled

Group Policy Processing

Relying on users to set group policies for their workstations creates the potential for users to inadvertently misconfigure or disable security functionality without consideration of the impact on the security posture of the workstation. Alternatively, an adversary could exploit this to disable any local group policies that are hampering their efforts to extract sensitive information. To reduce this risk, all audit, user rights and security related group policy settings should be specified for workstations at an organisational unit or domain level. To ensure these policies aren't weakened, support for local group policies should also be disabled.

The following group policies can be implemented to ensure only domain-based group policy settings are applied to workstations.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\System\Group Policy	
Configure registry policy processing	Enabled Process even if the Group Policy objects have not changed

Group Policy	Recommended Value
Configure security policy processing	Enabled Process even if the Group Policy objects have not changed
Remove users' ability to invoke machine policy refresh	Enabled
Set Group Policy refresh interval for computers	Enabled This setting allows you to customize how often Group Policy is applied to computers. The range is 0 to 64800 minutes (45 days). Minutes: 90 This is a random time added to the refresh interval to prevent all clients from requesting Group Policy at the same time. The range is 0 to 1440 minutes (24 hours). Minutes: 30
Turn off background refresh of Group Policy	Disabled
Turn off Local Group Policy Objects processing	Enabled

Built-in Guest Accounts

When built-in guest accounts are used it can allow an adversary to log onto a workstation over the network without first needing to compromise legitimate user credentials. To reduce this risk, built-in guest accounts should be disabled.

The following group policies can be implemented to disable and rename built-in guest accounts.

Group Policy	Recommended Value
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Accounts: Guest account status	Disabled
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment	
Deny log on locally	Guests

Microsoft Accounts

A new feature of Microsoft Windows 8 is the ability to link Microsoft accounts (formerly Windows Live IDs) to local or domain accounts. When this occurs, a user's settings and files are stored in the cloud using OneDrive rather than locally or on a domain controller. While this may have the benefit of allowing users to access their settings and files from any Microsoft Windows 8 workstation (e.g.

corporate workstation, home PC, Internet café) it can also pose a risk to an organisation as they lose control over where sensitive information may be accessed from. To reduce this risk, users should not link Microsoft accounts with local or domain accounts.

The following group policies can be implemented to disable the ability to link Microsoft accounts to local or domain accounts.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\Windows Components\OneDrive	
Prevent the usage of OneDrive for file storage	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Sync your settings	
Do not sync	Enabled
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Accounts: Block Microsoft accounts	Users can't add or log on with Microsoft accounts

Password Policy

The use of weak passwords, such as eight character passwords with no complexity, can allow them to be brute forced within minutes using applications freely available on the Web. In addition, having no maximum password age can allow an adversary to maintain extended access to a workstation or network once a password has been compromised while having no minimum password age can allow an adversary to recycle passwords if forced to change them due to maximum password ages. To reduce this risk, a secure password policy should be implemented.

The following group policies can be implemented to achieve a secure password policy.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\System\Logon	
Turn off picture password sign-in	Enabled
Turn on PIN sign-in	Disabled
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy	
Enforce password history	8 passwords remembered
Maximum password age	90 days
Minimum password age	1 days
Minimum password length	10 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Accounts: Limit local account use of blank passwords to console logon only	Enabled

Group Policy	Recommended Value
Interactive logon: Prompt user to change password before expiration	14 days

Account Lockout Policy

Allowing unlimited attempts to access workstations will fail to prevent an adversary's attempts to brute force authentication measures. To reduce this risk, accounts should be locked out after a defined number of invalid authentication attempts. The threshold for locking out accounts does not need to be overly restrictive in order to be effective. For example, a threshold of 5 incorrect attempts, with a reset period of 30 minutes, will prevent any brute force attempt while being unlikely to lock out a legitimate user who accidently enters their password incorrectly a few times.

The following group policies can be implemented to achieve a reasonable lockout policy.

Group Policy	Recommended Value
Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy	
Account lockout duration	0
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	30 minutes

NoLMHash Policy

When Microsoft Windows hashes a password that is less than 15 characters, it stores both a LAN Manager hash (LM hash) and Windows NT hash (NT hash) in the local SAM database for local accounts, or in Activity Directory for domain accounts. The LM hash is significantly weaker than the NT hash and can easily be brute forced. To reduce this risk, the NoLMHash Policy should be implemented on all workstations and domain controllers. As the LM hash is designed for authentication of legacy Microsoft Windows operating systems, such as those prior to Microsoft Windows 2000, there shouldn't be a business requirements for its use except in very rare circumstances.

The following group policy can be implemented to prevent the storage of LM hashes for passwords. All users should be encouraged to change their password once this group policy has been set as until they do they will remain vulnerable.

Group Policy	Recommended Value
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Network security: Do not store LAN Manager hash value on next password change	Enabled

Credential Entry

When users enter their credentials on a workstation it provides an opportunity for malicious code, such as a key logging application, to capture the credentials. To reduce this risk, users should be authenticated by using a trusted path to enter their credentials on the Secure Desktop.

The following group policies can be implemented to ensure credentials are entered in a secure manner as well as prevent the disclosure of usernames of previous users.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\System\Logon	
Do not enumerate connected users on domain-joined computers	Enabled
Enumerate local users on domain-joined computers	Disabled
Hide entry points for Fast User Switching	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Credential User Interface	
Do not display the password reveal button	Enabled
Enumerate administrator accounts on elevation	Disabled
Require trusted path for credential entry	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Logon Options	
Disable or enable software Secure Attention Sequence	Disabled
Display information about previous logons during user logon	Enabled
Report when logon server was not available during user logon	Enabled
Sign-in last interactive user automatically after a system-initiated restart	Disabled
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Interactive logon: Do not display last user name	Enabled
Interactive logon: Do not require CTRL + ALT + DEL	Disabled

Credential Caching

Cached credentials can allow a user to log onto a workstation they have previously logged onto even if the domain is not available. This functionality can be abused by an adversary who can retrieve these cached credentials. To reduce this risk, cached credentials should not be stored for workstations and only one previous logon should be cached for mobile users.

The following group policies can be implemented to disable credential caching.

Group Policy	Recommended Value
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	0 logons
Network access: Do not allow storage of passwords and credentials for network authentication	Enabled

Elevating Privileges

Microsoft Windows provides the ability to require confirmation from users, via the User Access Control (UAC) functionality, before any sensitive actions are performed. The default settings allow privileged users to perform sensitive actions without first providing credentials and while standard users must provide privileged credentials they are not required to do so via a trusted path on the Secure Desktop. This provides an opportunity for an adversary that gains access to an open session of a privileged user to perform sensitive actions at will or for malicious code to capture any credentials entered via a standard user when attempting to elevate their privileges. To reduce this risk, UAC functionality should be implemented to ensure all sensitive actions are authorised by providing credentials on the Secure Desktop.

The following group policies can be implemented to configure UAC functionality effectively.

Group Policy	Recommended Value
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
User Account Control: Admin Approval Mode for the Built-in Administrator account	Enabled
User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop	Disabled
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for credentials on the secure desktop
User Account Control: Behavior of the elevation prompt for standard users	Prompt for credentials on the secure desktop
User Account Control: Detect application installations and prompt for elevation	Enabled
User Account Control: Only elevate executables that are signed and validated	Disabled
User Account Control: Only elevate UIAccess applications that are installed in secure locations	Enabled
User Account Control: Run all administrators in Admin Approval Mode	Enabled
User Account Control: Switch to the secure desktop when prompting for elevation	Enabled
User Account Control: Virtualize file and registry write failures to per-user locations	Enabled

Autoplay and AutoRun

When enabled, Autoplay will automatically begin reading from a drive or media source as soon as it is used with a workstation, while AutoRun commands, generally in an autorun.inf file on the media, can be used to automatically execute any file on the media without user interaction. This functionality can be exploited by an adversary to automatically execute malicious code. To reduce this risk, Autoplay and AutoRun functionality should be disabled.

The following group policies can be implemented to disable Autoplay and AutoRun functionality.

Group Policy	Recommended Value

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\Windows Components\AutoPlay Policies	
Disallow Autoplay for non-volume devices	Enabled
Set the default behavior for AutoRun	Enabled Default AutoRun Behavior: Do not execute any autorun commands
Turn off Autoplay	Enabled Turn off Autoplay on: All drives

Endpoint Device Control

An adversary with physical access to a workstation may attempt to connect unauthorised USB media or other devices with mass storage functionality (e.g. smartphones, digital music players or cameras) to facilitate malicious code infections or the unauthorised copying of sensitive information. To reduce this risk, endpoint device control functionality should be appropriately implemented to control the use of all removable storage devices.

The following group policy can be implemented to disable the use of removable storage devices.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\System\Removable Storage Access	
All Removable Storage classes: Deny all access	Enabled

Alternatively, if specific classes of removable storage devices are required to meet business requirements, the execute, read and write permissions should be controlled on a class by class basis.

The following group policies provide a sample implementation that allows data to be read from but not executed from or written to all classes of removable storage devices.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\System\Removable Storage Access	
CD and DVD: Deny execute access	Enabled
CD and DVD: Deny read access	Disabled
CD and DVD: Deny write access	Enabled
Custom Classes: Deny read access	Disabled
Custom Classes: Deny write access	Enabled
Floppy Drives: Deny execute access	Enabled
Floppy Drives: Deny read access	Disabled
Floppy Drives: Deny write access	Enabled

Group Policy	Recommended Value
Removable Disks: Deny execute access	Enabled
Removable Disks: Deny read access	Disabled
Removable Disks: Deny write access	Enabled
Tape Drives: Deny execute access	Enabled
Tape Drives: Deny read access	Disabled
Tape Drives: Deny write access	Enabled
WPD Devices: Deny read access	Disabled
WPD Devices: Deny write access	Enabled

Administrative Shares

Administrative shares can allow an adversary that has compromised either local or domain privileged credentials to transfer malicious code between workstations. This can be used in conjunction with remote scheduling or remote registry access and run lists to execute malicious code on a targeted workstation. To reduce this risk, administrative shares such as C$ and ADMIN$ should be disabled.

The following group policies can be implemented to disable administrative shares on servers and workstations.

Group Policy	Recommended Value
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
MSS: (AutoShareServer) Enable Administrative Shares (recommended except for highly secure environments)	Disabled
MSS: (AutoShareWks) Enable Administrative Shares (recommended except for highly secure environments)	Disabled

File and Print Sharing

Users sharing files from their workstations can result in a lack of appropriate access controls being applied to sensitive information and the potential for the propagation of malicious code should file shares have read/write access. To reduce this risk, local file and print sharing should be disabled. Ideally, sensitive information should be centrally managed (e.g. on a network share with appropriate access controls). Disabling file and print sharing will not affect a user's ability to access shared drives and printers on a network.

The following group policies can be implemented to prevent users from sharing files.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\Network\Microsoft Peer-to-Peer Networking Services	
Turn off Microsoft Peer-to-Peer Networking Services	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\HomeGroup	

Group Policy	Recommended Value
Prevent the computer from joining a homegroup	Enabled
User Configurations\Policies\Administrative Templates\Windows Components\Network Sharing	
Prevent users from sharing files within their profile.	Enabled

Remote Desktop Services

While remote desktop access may be convenient for legitimate users to access workstations across a network, it also allows an adversary to access other workstations once they have compromised an initial workstation and user's credentials. This risk can be compounded if an adversary can compromise domain administrator credentials or common local administrator credentials. To reduce this risk, Remote Desktop Services should be disabled.

The following group policies can be implemented to disable Remote Desktop Services.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections	
Allow users to connect remotely by using Remote Desktop Services	Disabled
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment	
Allow log on through Remote Desktop Services	*<blank>*
Deny log on through Remote Desktop Services	Administrators Guests

Alternatively, if it is an essential business requirement to use Remote Desktop Services, it should be configured in a manner that is as secure as possible and only on workstations and for users for which it is explicitly required.

The following group policies can be implemented to use Remote Desktop Services in as secure a manner as possible.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Connection Client	
Allow .rdp files from unknown publishers	Disabled
Allow .rdp files from valid publishers and user's default .rdp settings	Enabled
Configure server authentication for client	Enabled Authentication setting: Do not connect if authentication fails
Do not allow passwords to be saved	Enabled

Group Policy	Recommended Value
Prompt for credentials on the client computer	Enabled
Specify SHA1 thumbprints of certificates representing trusted .rdp publishers	Enabled Comma-separated list of SHA1 trusted certificate thumbprints:*<as required>*
Turn Off UDP On Client	Disabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections	
Allow users to connect remotely by using Remote Desktop Services	Enabled
Automatic reconnection	Enabled
Configure keep-alive connection interval	Disabled
Deny logoff of an administrator logged in to the console session	Enabled
Limit number of connections	Enabled RD Maximum Connections allowed: *<organisation defined>*
Restrict Remote Desktop Services users to a single Remote Desktop Services session	Enabled
Select network detection on the server	Enabled Select Network Detect Level: Use both Connect Time Detect and Continuous Network Detect
Select RDP transport protocols	Enabled Select Transport Type: Use both UDP and TCP
Suspend user sign-in to complete app registration	Disabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection	
Do not allow Clipboard redirection	Enabled
Do not allow drive redirection	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security	
Always prompt for password upon connection	Enabled
Do not allow local administrators to customize permissions	Enabled

Group Policy	Recommended Value
Require secure RPC communication	Enabled
Require use of specific security layer for remote (RDP) connections	Enabled Security Layer: SSL (TLS 1.0)
Require user authentication for remote connections by using Network Level Authentication	Enabled
Server authentication certificate template	Not configured
Set client connection encryption level	Enabled Encryption Level: High Level
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Session Time Limits	
End session when time limits are reached	Enabled
Set time limit for active but idle Remote Desktop Services sessions	Enabled Idle session limit: 15 minutes
Set time limit for active Remote Desktop Services sessions	Enabled Active session limit: 2 hours
Set time limit for disconnected sessions	Enabled End a disconnected session: 1 minute
Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Temporary folders	
Do not delete temp folders upon exit	Disabled
Do not use temporary folders per session	Disabled
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment	
Allow log on through Remote Desktop Services	Remote Desktop Users
Deny log on through Remote Desktop Services	Administrators Guests

Concurrent Sessions

While the default state for the desktop line of Microsoft Windows operating systems is to not allow concurrent sessions, hacks exist on the Web for enabling concurrent sessions (i.e. by modifying termsrv.dll). Enabling concurrent sessions can allow an adversary with compromised credentials to silently connect to a workstation running Remote Desktop Services rather than having to forcibly logoff

a user already logged in, an activity that users should be aware to report to system administrators as suspicious behaviour. To reduce this risk, Microsoft Windows should not be hacked to enable the ability to use concurrent sessions.

Remote Assistance

While Remote Assistance can be a useful business tool to allow system administrators to remotely administer workstations, it can also pose a risk. When a user has a problem with their workstation they can generate a Remote Assistance invitation. This invitation authorises anyone that has access to it to remotely control the workstation that issued the invitation. Invitations can be sent by email, instant messaging or saved to a file. If an adversary manages to intercept an invitation they will be able to use it to access the user's workstation. Additionally, if network traffic on port 3389 is not blocked from reaching the Internet, users may send Remote Assistance invitations over the Internet which could allow for remote access to their workstation by an adversary. While Remote Assistance only grants access to the privileges of the user that generated the request, an adversary could install a key logging application on the workstation in preparation of a system administer using their privileged credentials to fix any problems. To reduce this risk, Remote Assistance should be disabled.

The following group policies can be implemented to disable Remote Assistance.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\System\Remote Assistance	
Configure Offer Remote Assistance	Disabled
Configure Solicited Remote Assistance	Disabled

Installing Applications

While the ability to install applications may be a business requirement for users, this privilege can be exploited by an adversary. An adversary can email a malicious application, or host a malicious application on a compromised website, and use social engineering techniques to convince users into installing the application on their workstation. Even if privileged access is required to install applications, users will use their privileged access if they believe, or can be convinced that, the requirement to install the application is legitimate. Additionally, if applications are configured to install using elevated privileges, an adversary can exploit this by creating a Windows Installer installation package to create a new account that belongs to the local built-in administrators group or to install a malicious application. To reduce this risk, all application installations should be strictly controlled.

The following group policies can be implemented to control the installation of applications.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer	
Configure Windows SmartScreen	Enabled Require approval from an administrator before running downloaded unknown software
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Installer	

Group Policy	Recommended Value
Allow user control over installs	Disabled
Allow users to browse for source while elevated	Disabled
Always install with elevated privileges	Disabled
Prevent Internet Explorer security prompt for Windows Installer scripts	Disabled
Turn off Windows Installer	Enabled Disable Windows Installer: For non-managed applications only
User Configuration\Policies\Administrative Templates\Windows Components\Windows Installer	
Always install with elevated privileges	Disabled

Legacy and Run Once Lists

Once malicious code has been copied to a workstation, an adversary with registry access can remotely schedule it to execute (i.e. using the run once list) or to automatically execute each time Microsoft Windows starts (i.e. using the legacy run list). To reduce this risk, legacy and run once lists should be disabled. This may interfere with the operation of legitimate applications that need to automatically execute each time Microsoft Windows starts. In such cases, the *Run these programs at user logon* group policy can be used to perform the same function in a more secure manner when defined at a domain level; however, if not used this group policy should be disabled rather than left in its default undefined state.

The following group policies can be implemented to disable the use of legacy and run once lists.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\System\Logon	
Do not process the legacy run list	Enabled
Do not process the run once list	Enabled
Run these programs at user logon	Disabled

Server Message Block Sessions

An adversary that has access to network communications may attempt to use session hijacking tools to interrupt, terminate or steal a Server Message Block (SMB) session. This could potentially allow an adversary to modify packets and forward them to a SMB server to perform undesirable actions or to pose as the server or client after a legitimate authentication has taken place to gain access to sensitive information. To reduce this risk, all communications between SMB clients and servers should be signed, with any passwords used appropriately encrypted.

The following group policies can be implemented to ensure communications between SMB clients and servers are secure.

Group Policy	Recommended Value
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Microsoft network client: Digitally sign communications (always)	Enabled
Microsoft network client: Digitally sign communications (if server agrees)	Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled
Microsoft network server: Amount of idle time required before suspending session	15 minutes
Microsoft network server: Attempt S4U2Self to obtain claim information	Default
Microsoft network server: Digitally sign communications (always)	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Enabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled
Microsoft network server: Server SPN target name validation level	Required from client

NetBIOS over TCP/IP

NetBIOS over TCP/IP facilitates a number of intrusion methods. To reduce this risk, NetBIOS over TCP/IP should be disabled. As NetBIOS over TCP/IP is only used to support legacy Microsoft Windows operating systems, such as those prior to Microsoft Windows 2000, there shouldn't be a business requirement for its use except in very rare circumstances. NetBIOS over TCP/IP can be disabled by setting the NetBIOS settings under the IPv4 WINS settings on each network interface to *Disable NetBIOS over TCP/IP*. NetBIOS over TCP/IP is not supported by IPv6.

Internet Protocol version 6

In Internet Protocol version 4 (IPv4) only networks, IPv6 functionality (enabled by default in Microsoft Windows 7 onwards), or IPv6 transition technologies, presents a security risk, especially when network security devices such as firewalls and IDS/IPSs aren't capable of filtering or auditing IPv6 traffic. This can allow an adversary to exploit vulnerabilities in IPv6 transition technologies or use IPv6 to bypass traditional IPv4 based filtering and auditing measures on the network. To reduce this risk, IPv6 functionality and IPv6 transition technologies should be disabled until all network security devices have been upgraded to support IPv6 and the organisation is ready to transition to IPv6.

The following group policies can be implemented to disable the use of IPv6 transition technologies while IPv6 functionality can be disabled within the properties of network interface cards installed in workstations.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\Network\TCPIP Settings\IPv6 Transition Technologies	
Set 6to4 State	Enabled Select from the following states: Disabled State

Group Policy	Recommended Value
Set IP-HTTPS State	Enabled Enter the IPHTTPS Url: http://localhost Select Interface state from the following options: Disabled State
Set ISATAP State	Enabled Select from the following states: Disabled State
Set Teredo State	Enabled Select from the following states: Disabled State

Signature-based Antivirus

When vendors develop software they often forgo secure coding practices or rush their products to market without sufficiently comprehensive testing. An adversary can take advantage of this to develop malicious code to exploit vulnerabilities in software not detected and remedied by the vendors. As significant time and effort is often involved in the development of functioning and reliable exploits, an adversary will often reuse their exploits as much as possible before being forced to develop new exploits by antivirus vendors that profile their exploits and develop detection signatures. Whilst exploits may be profiled by antivirus vendors, they often remain a viable intrusion method in organisations that don't have any measures in place to detect them. To reduce this risk, endpoint security applications with signature-based antivirus functionality should be appropriately implemented. In doing so, signatures should be updated at least on a daily basis.

Hard Drive Encryption

An adversary with physical access to a workstation may be able to use a bootable CD/DVD or USB media to load their own operating environment. From this environment, they can access the local file system to gain access to sensitive information or the SAM database to access password hashes. In addition, an adversary that gains access to a stolen or unsanitised hard drive will be to recover its contents when connected to another machine on which they have administrative access and can take ownership of files. To reduce this risk, hardware-based (TCG Opal 2.0 certified) 256-bit AES full disk encryption, ideally with Active Directory authentication support, should be used to protect the contents of hard drives from unauthorised access. Failing this, software-based 128-bit AES full disk encryption can be used as a minimum standard.

If Microsoft BitLocker is used for hard drive encryption, the following group policies can be implemented as a suitable baseline.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption	
Choose default folder for recovery password	Not configured

Group Policy	Recommended Value
Choose drive encryption method and cipher strength	Enabled Select the encryption method: AES 256-bit
Prevent memory overwrite on restart	Disabled
Provide the unique identifiers for your organization	Not configured
Validate smart card certificate usage rule compliance	Not configured
Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives	
Allow access to BitLocker-protected fixed data drives from earlier versions of Windows	Disabled
Choose how BitLocker-protected fixed drives can be recovered	Enabled Omit recovery options from the BitLocker setup wizard Save BitLocker recovery information to AD DS for fixed data drives Configure storage of BitLocker recovery information to AD DS: Backup recovery passwords and key packages Do not enable BitLocker until recovery information is stored to AD DS for fixed data drives
Configure use of hardware-based encryption for fixed data drives	Disabled
Configure use of passwords for fixed data drives	Enabled Require password for fixed data drive Configure password complexity for fixed data drives: Require password complexity Minimum password length for fixed data drive: 10
Configure use of smart cards on fixed data drives	Disabled
Deny write access to fixed drives not protected by BitLocker	Enabled

Group Policy	Recommended Value
Enforce drive encryption type on fixed data drive	Enabled Select the encryption type: Full encryption
Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives	
Allow enhanced PINs for startup	Enabled
Allow network unlocked at startup	Enabled
Allow Secure Boot for integrity validation	Enabled
Choose how BitLocker-protected operating system drives can be recovered	Enabled Omit recovery options from the BitLocker setup wizard Save BitLocker recovery information to AD DS for fixed data drives Configure storage of BitLocker recovery information to AD DS: Backup recovery passwords and key packages Do not enable BitLocker until recovery information is stored to AD DS for operating system drives
Configure minimum PIN length for startup	Enabled Minimum characters: 10
Configure TPM platform validation profile for BIOS-based firmware configurations	Enabled PCR 0 PCR 2 PCR 4 PCR 8 PCR 9 PCR 10 PCR 11

Group Policy	Recommended Value
Configure TPM platform validation profile for native UEFI firmware configurations	Enabled PCR 0 PCR 2 PCR 4 PCR 7 PCR 11
Configure use of hardware-based encryption for operating system drives	Disabled
Configure use of passwords for operating system drives	Enabled Configure password complexity for operating system drives: Require password complexity Minimum password length for operating system drive: 10
Disallow standard users from changing the PIN or password	Disabled
Enable use of BitLocker authentication requiring preboot keyboard input on slates	Enabled
Enforce drive encryption type on operating system drive	Enabled Select the encryption type: Full encryption
Require additional authentication at startup	Enabled Settings for computers with a TPM Configure TPM startup: Do not allow TPM Configure TPM startup PIN: Require startup PIN with TPM Configure TPM startup key: Do not allow startup key with TPM Configure TPM startup key and PIN: Do not allow startup key and PIN with TPM
Reset platform validation data after BitLocker recovery	Enabled

Group Policy	Recommended Value
Use enhanced Boot Configuration Data validation profile	Not configured
Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives	
Allow access to BitLocker-protected removable data drives from earlier versions of Windows	Disabled
Choose how BitLocker-protected removable drives can be recovered	Enabled Omit recovery options from the BitLocker setup wizard Save BitLocker recovery information to AD DS for removable data drives Configure storage of BitLocker recovery information to AD DS: Backup recovery passwords and key packages Do not enable BitLocker until recovery information is stored to AD DS for removable data drives
Configure use of hardware-based encryption for removable data drives	Disabled
Configure use of passwords for removable data drives	Enabled Require password for removable data drive Configure password complexity for removable data drives: Require password complexity Minimum password length for removable data drive: 10
Configure use of smart cards on removable data drives	Disabled
Control use of BitLocker on removable drives	Enabled Allow users to apply BitLocker protection on removable data drives
Deny write access to removable drives not protected by BitLocker	Enabled

Group Policy	Recommended Value
Enforce drive encryption type on removable data drive	Enabled Select the encryption type: Full encryption
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Interactive logon: Machine account lockout threshold	10 invalid logon attempts

Direct Memory Access

Communications interfaces that use Direct Memory Access (DMA) can allow an adversary with physical access to a workstation to directly access the contents of a workstation's memory. This can be used to read sensitive contents such as cryptographic keys or to write malicious code directly into memory. To reduce this risk, communications interfaces that allow DMA (e.g. FireWire and Thunderbolt) should be disabled. This can be achieved either physically (e.g. using epoxy) or by using software controls[21] (e.g. disabling the functionality in the Basic Input/Output System (BIOS) or UEFI; removing the SBP-2 driver and disabling the Thunderbolt controller; or using an end point protection solution).

Power Management

One method of reducing power usage by workstations is to enter a sleep, hibernation or hybrid sleep state after a pre-defined period of inactivity. When a workstation enters a sleep state it maintains the contents of memory while powering down the rest of the workstation; with hibernation or hybrid sleep, it writes the contents of memory to the hard drive in a hibernation file (hiberfil.sys) and powers down the rest of the workstation. When this occurs, sensitive information such as encryption keys could either be retained in memory or written to the hard drive in a hibernation file. An adversary with physical access to the workstation and either the memory or hard drive can recover the sensitive information using forensic techniques. To reduce this risk, sleep, hibernation and hybrid sleep states should be disabled.

The following group policies can be implemented to ensure that sleep, hibernation and hybrid sleep states are disabled.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings	
Allow standby states (S1-S3) when sleeping (on battery)	Disabled
Allow standby states (S1-S3) when sleeping (plugged in)	Disabled
Require a password when a computer wakes (on battery)	Enabled
Require a password when a computer wakes (plugged in)	Enabled
Specify the system hibernate timeout (on battery)	Enabled System Hibernate Timeout (seconds): 0

Group Policy	Recommended Value
Specify the system hibernate timeout (plugged in)	Enabled System Hibernate Timeout (seconds): 0
Specify the system sleep timeout (on battery)	Enabled System Sleep Timeout (seconds): 0
Specify the system sleep timeout (plugged in)	Enabled System Sleep Timeout (seconds): 0
Specify the unattended sleep timeout (on battery)	Enabled Unattended Sleep Timeout (seconds): 0
Specify the unattended sleep timeout (plugged in)	Enabled Unattended Sleep Timeout (seconds): 0
Turn off hybrid sleep (on battery)	Enabled
Turn off hybrid sleep (plugged in)	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer	
Show hibernate in the power options menu	Disabled
Show sleep in the power options menu	Disabled

System Cryptography

By default, when cryptographic keys are stored in Microsoft Windows, users can access them without first entering a password to unlock the certificate store. An adversary that compromises a workstation, or gains physical access to an unlocked workstation, can use these user keys to access sensitive information or resources that are cryptographically protected. To reduce this risk, strong encryption algorithms and strong key protection should be used on workstations.

The following group policies can be implemented to ensure strong encryption algorithms and strong key protection is used.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\System\Filesystem\NTFS	
Do not allow encryption on all NTFS volumes	Disabled
Enable NTFS pagefile encryption	Enabled
Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings	

Group Policy	Recommended Value
Turn off Automatic Root Certificate Update	Disabled
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
System cryptography: Force strong key protection for user keys stored on the computer	User must enter a password each time they use a key
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Enabled

Registry Editing Tools

One method for malicious code to maintain persistence (i.e. remain after a workstation is rebooted) is to use administrative privileges to modify the registry (as standard privileges only allow viewing of the registry). To reduce this risk, users should not have the ability to modify the registry using registry editing tools (i.e. regedit) or to make silent changes to the registry (i.e. using .reg files).

The following group policy can be implemented to prevent users from viewing or modifying the registry using registry editing tools.

Group Policy	Recommended Value
User Configuration\Policies\Administrative Templates\System	
Prevent access to registry editing tools	Enabled Disable regedit from running silently: Yes

Windows Remote Shell Access

When Windows Remote Shell is enabled it can allow an adversary to remotely execute scripts and commands on workstations. To reduce this risk, Windows Remote Shell should be disabled.

The following group policy can be implemented to disable Windows Remote Shell access.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Shell	
Allow Remote Shell Access	Disabled

Boot Devices

By default workstations are often configured to boot from optical media, or even USB media, in preference to hard drives. An adversary with physical access to such workstations can boot from their own media in order to gain access to the content of the hard drives. With this access an adversary can reset local user account passwords or gain access to the local SAM database to steal password hashes for offline brute force cracking attempts. To reduce this risk, workstations should be restricted to only booting from the designated primary system drive.

BIOS and UEFI Passwords

An adversary with access to a workstation's BIOS or UEFI can modify the hardware configuration of the workstation to introduce attack vectors or weaken security functionality within the workstation's operating system. This can include disabling security functionality in the CPU, modifying allowed boot devices and enabling insecure communications interfaces such as FireWire and Thunderbolt. To reduce this risk, strong BIOS and UEFI passwords should be used for all workstations to prevent unauthorised access.

Case Locks

Without the use of case locks an adversary can gain physical access to the insides of a workstation. An adversary with this access can install or remove hardware, remove and replace the CMOS battery to reset the BIOS or UEFI to default settings (i.e. no password), or temporarily remove hard drives to create copies for offline analysis at a later date. To reduce this risk, case locks should be used on workstations to prevent an adversary from gaining unauthorised access.

Recovery Console

An adversary that has physical access to a workstation may attempt to access the recovery console using a Microsoft Windows installation disc or by causing an error state in the operating system by directly removing power while it is running. As the recovery console automatically logs on as an administrator by default, an adversary may use this to access any content on the workstation (i.e. using the *set AllowAllPaths=true* command), write any content to removable media (i.e. using the *set AllowRemovableMedia=true* command) or overwrite any file without leaving any traces. To reduce this risk, automatic logon and the use of the *set* command for the recovery console should be disabled.

The following group policies can be implemented to disable automatic logon and the *set* command for the recovery console.

Group Policy	Recommended Value
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled

Safe Mode

An adversary with standard user credentials that can boot into Microsoft Windows using Safe Mode, Safe Mode with Networking or Safe Mode with Command Prompt options may be able to bypass system protections and security functionality such as application whitelisting solutions. To reduce this risk, users with standard credentials should be prevented from using Safe Mode options to log in.

The following registry entry can be implemented to prevent non-administrators from using Safe Mode options.

Registry Entry	Recommended Value
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System	
SafeModeBlockNonAdmins	REG_DWORD 0x00000001 (1)

Session Locking

An adversary with physical access to an unattended workstation may attempt to inappropriately access other users' sessions in order to use their credentials to access sensitive information they don't have access to or to conduct actions on the network that won't be attributed to them. To reduce this risk, a session lock should be configured to activate after a maximum of 15 minutes of user inactivity.

The following group policies can be implemented to set session locks.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\System\Logon	
Allow users to select when a password is required when resuming from connected standby	Disabled
Turn off app notifications on the lock screen	Enabled
Computer Configuration\Policies\ Administrative Templates\Windows Components\File Explorer	
Show lock in the user tile menu	Enabled
Computer Configuration\Policies\Windows Settings\Local Policies\Security Options	
Interactive logon: Display user information when the session is locked	User display name only
Interactive logon: Machine inactivity limit	900 seconds
Interactive logon: Require Domain Controller authentication to unlock workstation	Enabled
MSS: (ScreenSaverGracePerod) The time in seconds before the screen saver grace period expires (0 recommended)	0
User Configuration\Policies\Administrative Templates\Control Panel\Personalization	
Enable screen saver	Enabled
Force specific screen saver	Enabled Screen saver executable name: *<organisation defined>*
Password protect the screen saver	Enabled
Prevent changing screen saver	Enabled
Screen saver timeout	Enabled Seconds: 900
User Configuration\Policies\Administrative Templates\Start Menu and Taskbar\Notifications	
Turn off toast notifications on the lock screen	Enabled

CD Burner Access

If CD burning functionality is enabled, and CD burners are installed in workstations, an adversary may attempt to steal sensitive information by burning it to CD. To reduce this risk, users should not have access to CD burning functionality except when explicitly required.

The following group policy can be implemented to prevent access to CD burning functionality, although as this group policy only prevents access to native CD burning functionality in Microsoft Windows, users should also be prevented from installing 3rd party CD burning applications. Alternatively, CD readers can be used in workstations instead of CD burners.

Group Policy	Recommended Value
User Configuration\Policies\Administrative Templates\Windows Components\File Explorer	
Remove CD Burning features	Enabled

Sound Recorder

Sound Recorder is a feature of Microsoft Windows that allows audio from a device with a microphone to be recorded and saved as an audio file on the local hard drive. An adversary with remote access to a workstation can use this functionality to record sensitive conversations in the vicinity of the workstation. To reduce this risk, Sound Recorder should be disabled.

The following group policy can be implemented to disable the use of Sound Recorder.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\Windows Components\Sound Recorder	
Do not allow Sound Recorder to run	Enabled

Legacy Applications

The ability to run 16-bit legacy applications on 32-bit (x86) versions of Microsoft Windows can present a number of vulnerabilities that can lead directly to elevation of privileges for an adversary. For example, Microsoft Security Bulletin MS13-063[22] resolved a publically disclosed vulnerability relating to 16-bit code execution that could bypass the ASLR security functionality within 32-bit (x86) versions of Microsoft Windows. To reduce this risk, 16-bit application support should be disabled unless specifically required to support legacy applications.

The following group policy can be implemented to disable 16-bit application support within 32-bit (x86) versions of Microsoft Windows.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\Windows Components\Application Compatibility	
Prevent access to 16-bit applications	Enabled

Windows To Go

A new feature of Microsoft Windows 8 is Windows To Go. Windows to Go allows users to boot into a Microsoft Windows 8 workspace stored on USB media from any machine that supports the minimum hardware requirements of Microsoft Windows 7 or Microsoft Windows 8. While this may be highly beneficial for Bring Your Own Device (BYOD) or remote access initiatives, it can also pose a risk to an

organisation's network. Workstations that allow automatic booting of Windows To Go workspaces do not discriminate between approved workspaces and malicious workspaces developed by an adversary. As such, an adversary may use a malicious workspace they have customised with their desired toolkit to attempt to gain access to sensitive information on the network. To reduce this risk, automatic booting of Windows to Go media should be disabled.

The following group policy can be implemented to disable the automatic booting of Windows to Go media.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\Windows Components\Portable Operating System	
Windows To Go Default Startup Options	Disabled

Anonymous Connections

An adversary can use anonymous connections to gather information about the state of workstations. Information that can be gathered from anonymous connections (i.e. using the *net use* command to connect to the IPC$ share) can include lists of users and groups, SIDs for accounts, lists of shares, workstation policies, operating system versions and security patch levels. To reduce this risk, anonymous connections to workstations should be disabled.

The following group policies can be implemented to disable the use of anonymous connections.

Group Policy	Recommended Value
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled
Network access: Let Everyone permissions apply to anonymous users	Disabled
Network access: Named Pipes that can be accessed anonymously	*<blank>*
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled
Network access: Shares that can be accessed anonymously	*<blank>*
Network access: Sharing and security model for local accounts	Classic - local users authenticate as themselves
Network security: Allow Local System to use computer identity for NTLM	Enabled
Network security: Allow LocalSystem NULL session fallback	Disabled
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment	
Access this computer from the network	Administrators
Deny access to this computer from the network	Guests

Group Policy	Recommended Value
Deny log on as a batch job	Guests
Deny log on as a service	Guests
Log on as a batch job	*<blank>*
Log on as a service	*<blank>*

Network Authentication

Using insecure network authentication methods may permit an adversary to gain unauthorised access to network traffic and services. To reduce this risk, only secure network authentication methods, ideally Kerberos, should be used for network authentication.

The following group policies can be implemented to enable Kerberos and disable the less secure NTLM authentication method.

Group Policy	Recommended Value
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Network security: Configure encryption types allowed for Kerberos	AES256_HMAC_SHA1
Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication	*<blank>*
Network security: Restrict NTLM: Add server exceptions in this domain	*<blank>*
Network security: Restrict NTLM: Audit Incoming NTLM Traffic	Disable
Network security: Restrict NTLM: Audit NTLM authentication in this domain	Disable
Network security: Restrict NTLM: Incoming NTLM traffic	Deny all accounts
Network security: Restrict NTLM: NTLM authentication in this domain	Deny all
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Deny all

Alternatively, if NTLM is deployed on the network, NTLMv2 and 128-bit encryption should be used.

The following group policies can be implemented to deploy NTLMv2 and 128-bit encryption.

Group Policy	Recommended Value
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Network security: LAN Manager authentication level	Send NTLMv2 response only. Refuse LM & NTLM
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Require NTLMv2 session security,Require 128-bit encryption
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Require NTLMv2 session security,Require 128-bit encryption

Secure Channel Communications

Periodically, workstations connected to a domain will communicate with the domain controllers. If an adversary has access to unprotected network communications they may be able to capture or modify sensitive information communicated between workstations and the domain controllers. To reduce this risk, all secure channel communications should be signed and encrypted with strong session keys.

The following group policies can be implemented to ensure secure channel communications are appropriately signed and encrypted.

Group Policy	Recommended Value
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled
Domain member: Digitally encrypt secure channel data (when possible)	Enabled
Domain member: Digitally sign secure channel data (when possible)	Enabled
Domain member: Require strong (Windows 2000 or later) session key	Enabled

Windows Connect Now

Windows Connect Now is a feature of Microsoft Windows that was introduced with Microsoft Windows Vista. Windows Connect Now is designed to use the Wi-Fi Protected Setup (WPS) protocol to connect workstations to networks. As numerous public vulnerabilities have been disclosed with WPS, its use presents a risk. To reduce this risk, Windows Connect Now should be disabled.

The following group policies can be implemented to disable Windows Connect Now.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\Network\Windows Connect Now	
Configuration of wireless settings using Windows Connect Now	Disabled
Prohibit access of the Windows Connect Now wizards	Enabled

Setting Network Location

In Microsoft Windows Vista administrative privileges were required to set or change the network location of workstations. However, with the introduction of Microsoft Windows 7 this was relaxed in favour of allowing standard users to set or change their network location. Users with the ability to change their network location could use this to bypass existing security functionality by connecting their workstation to a less secure network environment. To reduce this risk, administrative privileges should be required to set the network location.

The following group policy can be implemented to enforce the use of administrative privileges for setting network locations.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\Network\Network Connections	
Require domain users to elevate when setting a network's location	Enabled

Bridging Networks

When workstations have multiple network interfaces, such as an Ethernet interface and a wireless interface, it is possible to establish a bridge between the connected networks. For example, when using an Ethernet interface to connect to an organisation's wired network and a wireless interface to connect to another non-organisation controlled network such as a public wireless hotspot. When bridges are created between such networks an adversary can directly access the wired network from the wireless network to extract sensitive information. To reduce this risk, the ability to install and configure network bridges between different networks should be disabled. This won't prevent an adversary from compromising a workstation via the wireless network and then using malicious software as a medium to indirectly access the wired network. This can only be prevented by manually disabling all wireless interfaces when connecting to wired networks.

The following group policies can be implemented to disable the ability to install and configure network bridges.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\Network\Network Connections	
Prohibit installation and configuration of Network Bridge on your DNS domain network	Enabled
Route all traffic through the internal network	Enabled Select from the following states: Enabled State
Computer Configuration\Policies\Administrative Templates\Network\Windows Connection Manager	
Prohibit connection to non-domain networks when connected to domain authenticated network	Enabled

Network Mapping

When a workstation is connected to a network that is defined as either *home* or *private* the Link-Layer Topology Discovery drivers can be used by the Microsoft Windows Network Map feature to create a graphical diagram of devices and connections for the local network. Such information could be used by an adversary to assist with network reconnaissance activities leading to the identification of key resources on the network. To reduce this risk, the LLTDIO and RSPNDR drivers should be disabled.

The following group policies can be implemented to disable the Link-Layer Topology Discovery drivers.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\Network\Link-Layer Topology Discovery	
Turn on Mapper I/O (LLTDIO) driver	Disabled
Turn on Responder (RSPNDR) driver	Disabled

Remote Procedure Call

Remote Procedure Call (RPC) is a technique used for facilitating client and server application communications using a common interface. RPC is designed to make client and server interaction easier and safer by using a common library to handle tasks such as security, synchronisation and data

flows. If unauthenticated communications are allowed between client and server applications, it could result in accidental disclosure of sensitive information or the failure to take advantage of RPC security functionality. To reduce this risk, all RPC clients should authenticate to RPC servers.

The following group policies can be implemented to ensure RPC clients authenticate to RPC servers.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\System\Remote Procedure Call	
Enable RPC Endpoint Mapper Client Authentication	Enabled
Restrict Unauthenticated RPC clients	Enabled RPC Runtime Unauthenticated Client Restriction to Apply: Authenticated without exceptions

Attachment Manager

The Attachment Manager within Microsoft Windows works in conjunction with applications such as Microsoft Outlook and Internet Explorer to help protect workstations from attachments that have been received via email or downloaded from the Web. The Attachment Manager classifies files as high, medium or low risk based on the zone they originated from and the type of file. Based on the risk to the workstation, the Attachment Manager will either issue a warning to a user or prevent them from opening a file. If zone information is not preserved, or can be removed, it can allow an adversary to bypass protections afforded by the Attachment Manager. To reduce this risk, the Attachment Manager should be configured to preserve and protect zone information for files.

The following group policies can be implemented to ensure zone information associated with attachments is preserved and protected.

Group Policy	Recommended Value
User Configuration\Policies\Administrative Templates\Windows Components\Attachment Manager	
Do not preserve zone information in file attachments	Disabled
Hide mechanisms to remove zone information	Enabled
Notify antivirus programs when opening attachments	Enabled

Command Prompt Access

An adversary who gains access to a workstation can use the command prompt to execute in-built Microsoft Windows tools such as *at* and *net* to gather information about the workstation or domain as well as schedule malicious code to execute on other workstations on the network. To reduce this risk, users should not have command prompt access or the ability to execute batch files and scripts. Should a legitimate business requirement exist to allow users to execute batch files (e.g. cmd and bat files); run logon, logoff, startup or shutdown batch file scripts; or use Remote Desktop Services, this risk will need to be accepted.

The following group policy can be implemented to prevent access to the command prompt and script processing functionality.

Group Policy	Recommended Value
User Configuration\Policies\Administrative Templates\System	
Prevent access to the command prompt	Enabled Disable the command prompt script processing also: Yes

PowerShell Scripts

Allowing any PowerShell script to execute exposes a workstation to the risk that a malicious script may be unwittingly executed by a user. To reduce this risk, users should not have the ability to execute PowerShell scripts; however, if using PowerShell scripts is an essential business requirement, only signed scripts should be allowed to execute. Ensuring that only signed scripts are allowed to execute can provide a level of assurance that a script is trusted and has been endorsed as having a legitimate business purpose.

The following group policy can be implemented to control the use of PowerShell scripts.

Registry Entry	Recommended Value
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows PowerShell	
Turn on Script Execution	Enabled Execution Policy: Allow only signed scripts

System Backup and Restore

An adversary that compromises a user account with privileges to backup files and directories can use this privilege to backup the contents of a workstation. This content can then be transferred to a non-domain connected workstation where the adversary has administrative access. From here an adversary can restore the contents and take ownership, thereby circumventing all original access controls that were in place. In addition, if a user has privileges to restore files and directories, an adversary could exploit this privilege by using it to either restore previous versions of files that may have been removed by system administrators as part of malicious code removal activities or to replace existing files with malicious variants. To reduce this risk, the ability to use backup and restore functionality should be disabled.

The following group policies can be implemented to prevent the use of backup and restore functionality.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\System\System Restore	
Turn off System Restore	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\File History	

Group Policy	Recommended Value
Turn off File History	Enabled
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment	
Back up files and directories	*<blank>*
Restore files and directories	*<blank>*

Security Configuration Editor Settings

By failing to specify MSS specific registry keys and values an adversary may be able to exploit weaknesses in a workstation's group policies to gain access to sensitive information. To reduce this risk, MSS specific registry keys and values should be comprehensively specified at a domain level. The LocalGPO command line tool bundled with the Microsoft Security Compliance Manager tool[23] provides the ability to add group policies for MSS specific registry keys and values. This can be done by running the command *cscript LocalGPO.wsf /ConfigSCE* from the LocalGPO command line.

The following group policies can be implemented to configure the MSS specific registry keys and values.

Group Policy	Recommended Value
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)	Disabled
MSS: (AutoReboot) Allow Windows to automatically restart after a system crash (recommended except for highly secure environments)	Disabled
MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)	Highest protection, source routing is completely disabled
MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)	Highest protection, source routing is completely disabled
MSS: (DisableSavePassword) Prevent the dial-up password from being saved (recommended)	Enabled
MSS: (EnableDeadGWDetect) Allow automatic detection of dead network gateways (could lead to DoS)	Disabled
MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes	Disabled
MSS: (Hidden) Hide Computer From the Browse List (not recommended except for highly secure environments)	Enabled
MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds	300000 or 5 minutes (recommended)

Group Policy	Recommended Value
MSS: (NoDefaultExempt) Configure IPSec exemptions for various types of network traffic.	Multicast, broadcast, & ISAKMP exempt (best for Windows XP).
MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers	Enabled
MSS: (NtfsDisable8dot3NameCreation) Enable the computer to stop generating 8.3 style filenames	Disable 8Dot3 Creation on all Volumes
MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)	Disabled
MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)	Enabled
MSS: (SynAttackProtect) Syn attack protection level (protects against DoS)	Connections time out sooner if a SYN attack is detected
MSS: (TcpMaxConenctResponseRetransmissions) SYN-ACK retransmissions when a connection request is not acknowledged	3 seconds, half-open connections dropped after 9 seconds
MSS: (TcpMaxDataRestransmissions IPv6) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)	3
MSS: (TcpMaxDataRestransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)	3

User Rights Policies

By failing to comprehensively specify user rights policies, an adversary may be able to exploit weaknesses in a workstation's group policies to gain access to sensitive information. To reduce this risk, user rights policies should be comprehensively specified.

The following group policies can be implemented, in addition to those specifically mentioned in other areas of this document, to form a comprehensive set of user rights policies.

Group Policy	Recommended Value
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment	
Access Credential Manager as a trusted caller	*<blank>*
Act as part of the operating system	*<blank>*
Add workstations to domain	Administrators
Adjust memory quotas for a process	Administrators LOCAL SERVICE NETWORK SERVICE

Group Policy	Recommended Value
Allow log on locally	Administrators Users
Bypass traverse checking	Administrators LOCAL SERVICE NETWORK SERVICE Users Windows Manager\ Windows Manager Group
Change the system time	Administrators LOCAL SERVICE
Change the time zone	Administrators LOCAL SERVICE
Create a pagefile	Administrators
Create a token object	*<blank>*
Create global objects	Administrators LOCAL SERVICE NETWORK SERVICE SERVICE
Create permanent shared objects	*<blank>*
Create symbolic links	Administrators
Debug programs	Administrators
Enable computer and user accounts to be trusted for delegation	*<blank>*
Force shutdown from a remote system	Administrators
Impersonate a client after authentication	Administrators LOCAL SERVICE NETWORK SERVICE SERVICE
Increase a process working set	Administrators LOCAL SERVICE Windows Manager\ Windows Manager Group
Increase scheduling priority	Administrators

Group Policy	Recommended Value
Load and unload device drivers	Administrators
Lock pages in memory	*<blank>*
Modify an object label	*<blank>*
Modify firmware environment values	Administrators
Perform volume maintenance tasks	Administrators
Profile single process	Administrators
Profile system performance	Administrators NT SERVICE\ WdiServiceHost
Remove computer from docking station	Administrators Users
Replace a process level token	LOCAL SERVICE NETWORK SERVICE
Shut down the system	Administrators Users
Synchronize directory service data	*<blank>*
Take ownership of files or other objects	Administrators

Security Policies

By failing to comprehensively specify security policies, an adversary may be able to exploit weaknesses in a workstation's group policies to gain access to sensitive information. To reduce this risk, security policies should be comprehensively specified.

The following group policies can be implemented, in addition to those specifically mentioned in other areas of this document, to form a comprehensive set of security policies.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer	
Turn off heap termination on corruption	Disabled
Turn off shell protocol protected mode	Disabled
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax	*<blank>*
DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax	*<blank>*

Group Policy	Recommended Value
Devices: Allow undock without having to log on	Enabled
Devices: Allowed to format and eject removable media	Administrators and Interactive Users
Devices: Prevent users from installing printer drivers	Enabled
Devices: Restrict CD-ROM access to locally logged-on user only	Enabled
Devices: Restrict floppy access to locally logged-on user only	Enabled
Domain controller: Allow server operators to schedule tasks	Disabled
Domain controller: LDAP server signing requirements	Require signing
Domain controller: Refuse machine account password changes	Disabled
Domain member: Disable machine account password changes	Disabled
Domain member: Maximum machine account password age	30 days
Interactive logon: Message text for users attempting to log on	*<organisation defined>*
Interactive logon: Message tile for users attempting to log on	*<organisation defined>*
Network access: Remotely accessible registry paths	System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications System\Microsoft\Windows NT\CurrentVersion

Group Policy	Recommended Value
Network access: Remotely accessible registry paths and sub-paths	System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ControlIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog
Network security: Allow PKU2U authentication requests to this computer to use online identities.	Disabled
Network security: Force logoff when logon hours expire	Enabled
Network security: LDAP client signing requirements	Negotiate signing
Shutdown: Allow system to be shut down without having to log on	Enabled
Shutdown: Clear virtual memory pagefile	Disabled
System objects: Require case insensitivity for non-Windows subsystems	Enabled
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled
System settings: Optional subsystems	*<blank>*

Group Policy	Recommended Value
System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies	Enabled

Low Severity Issues

An issue of low severity indicates a poorly configured setting or discusses an issue that in conjunction with another identified issue may result in a larger residual risk to a workstation.

Resultant Set of Policy Reporting

By default, all users have the ability to generate Resultant Set of Policy (RSOP) reports which allows them to view the group policies being applied to their workstation and user account. This information could be used by an adversary to determine misconfigurations or weaknesses in group policies being applied to the workstation or the user account. To reduce this risk, users should not have the ability to generate RSOP reports.

The following group policy can be implemented to disable users' ability to generate RSOP reports.

Group Policy	Recommended Value
User Configuration\Policies\Administrative Templates\System\Group Policy	
Determine if interactive users can generate Resultant Set of Policy data	Enabled

Displaying File Extensions

When extensions for known file types are hidden, an adversary can more easily use social engineering techniques to convince users to execute malicious email attachments. For example, a file named *vulnerability_assessment.pdf.exe* could appear as *vulnerability_assessment.pdf* to a user. To reduce this risk, hiding extensions for known file types should be disabled. Showing extensions for all known file types, in combination with user education and awareness of dangerous email attachment file types, can help reduce the risk of users executing malicious email attachments.

The following registry entry can be implemented to prevent extensions for known file types from being hidden.

Registry Entry	Recommended Value
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	
HideFileExt	REG_DWORD 0x00000000 (0)

Location Awareness

When users interact with the Internet their workstations often automatically provide geo-location details to websites or online services to assist them in tailoring content specific to the user's geographical region (i.e. the city they are accessing the Internet from). This information can be captured by an adversary to determine the location of a specific user. To reduce this risk, location services in the operating system and applications should be disabled.

The following group policies can be implemented to disable location services within the operating system.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\Windows Components\Location and Sensors	
Turn off location	Enabled

Group Policy	Recommended Value
Turn off location scripting	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Location and Sensors\Windows Location Provider	
Turn off Windows Location Provider	Enabled

Reporting System Information

Microsoft Windows contains a number of in-built functions to, often automatically and transparently, report system information to Microsoft. This includes driver errors; handwriting samples; file types associated with applications; user surveys; system errors and crash information; system performance information; and inventories of applications, files, devices and drivers on the system. If captured by an adversary, this information could expose sensitive information on workstations such as file names, directory names or versions of installed applications. This information could subsequently be used by an adversary to tailor malicious code to target specific workstations or users. To reduce this risk, all in-built functions that report system information to Microsoft should be disabled.

The following group policies can be implemented to prevent system information being reported to Microsoft.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\System\Device Installation	
Do not send a Windows error report when a generic driver is installed on a device	Enabled
Prevent device metadata retrieval from the Internet	Enabled
Prevent Windows from sending an error report when a device driver requests additional software during installation	Enabled
Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings	
Turn off Event Viewer “Events.asp” links	Enabled
Turn off handwriting personalization data sharing	Enabled
Turn off handwriting recognition error reporting	Enabled
Turn off Help and Support Center “Did you know?” content	Enabled
Turn off Help and Support Center Microsoft Knowledge Base search	Enabled
Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com	Enabled
Turn off Registration if URL connection is referring to Microsoft.com	Enabled
Turn off Search Companion content file updates	Enabled
Turn off the Windows Messenger Customer Experience Improvement Program	Enabled

Group Policy	Recommended Value
Turn off the Windows Customer Experience Improvement Program	Enabled
Turn off Windows Error Reporting	Enabled
Computer Configuration\Policies\Administrative Templates\System\Troubleshooting and Diagnostics\Microsoft Support Diagnostic Tool	
Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider	Disabled
Computer Configuration\Policies\Administrative Templates\System\Troubleshooting and Diagnostics\Scripted Diagnostics	
Troubleshooting: Allow users to access online troubleshooting content on Microsoft servers from the Troubleshooting Control Panel (via the Windows Online Troubleshooting Service – WOTS)	Disabled
Computer Configuration\Policies\Administrative Templates\System\Troubleshooting and Diagnostics\Windows Performance PerfTrack	
Enable/Disable PerfTrack	Disabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Application Compatibility	
Turn off Application Telemetry	Enabled
Turn off Inventory Collector	Enabled
Turn off Steps Recorder	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender\MAPS	
Join Microsoft MAPS	Enabled Join Microsoft MAPS: Disabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Error Reporting	
Automatically send memory dumps for OS-generated error reports	Disabled
Disable Windows Error Reporting	Enabled
Do not send additional data	Enabled
Prevent display of the user interface for critical errors	Enabled
User Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings	
Turn off Help Experience Improvement Program	Enabled
Turn off Help Ratings	Enabled

Microsoft Store

Whilst applications in the Microsoft Store are vetted by Microsoft, there is still a risk that users given access to the Microsoft Store could download and install potentially malicious applications or applications that cause conflicts with other endorsed applications on their workstation. To reduce this risk, access to the Microsoft Store should be disabled.

The following group policies can be implemented to prevent Microsoft Store access.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings	
Turn off access to the Store	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Digital Locker	
Do not allow Digital Locker to run	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Store	
Turn off the Store application	Enabled

File and Folder Security Properties

By default, all users have the ability to view security properties of files and folders. This includes the security properties associated with files and folders as well as users and groups that they relate to. An adversary could use this information to target specific accounts that have access to sensitive information. To reduce this risk, users should not have the ability to view security properties of files and folders.

The following group policy can be implemented to disable users' access to the security tab in file and folder properties in File Explorer.

Group Policy	Recommended Value
User Configuration\Policies\Administrative Templates\Windows Components\File Explorer	
Remove Security tab	Enabled

Web Searching

As part of the in-built search functionality of Microsoft Windows, users can search for Web results in addition to local workstation results. This functionality if used could result in the accidental disclosure of sensitive information if sensitive terms are searched for automatically on the Web in addition to the local workstation. To reduce this risk, the ability to automatically search the Web should be disabled.

The following group policies can be implemented to prevent Web search results being returned for any user search terms.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\Windows Components\Search	
Don't search the web or display web results in Search	Enabled

Group Policy	Recommended Value
Don’t search the web or display web results in Search over metered connections	Enabled

Internet Printing

Microsoft Windows has the ability to print to Internet printers over HTTP. If not disabled, this functionality could result in the accidental or intentional release of sensitive information into the public domain. To reduce this risk, Internet printing should be disabled.

The following group policies can be implemented to prevent the use of Internet printing.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings	
Turn off downloading of print drivers over HTTP	Enabled
Turn off printing over HTTP	Enabled

Publishing Information to the Web

Microsoft Windows has the ability to assist users in either directly publishing information to the Web or sending information to publishers for professional publication. If not disabled, this functionality could result in the accidental or intentional release of sensitive information into the public domain. To reduce this risk, the ability to publish information to the Web or send to publishers should be disabled.

The following group policies can be implemented to disable the ability to publish information to the Web or send it to publishers.

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings	
Turn off Internet download for Web publishing and online ordering wizards	Enabled
Turn off the “Order Prints” picture task	Enabled
Turn off the “Publish to Web” task for files and folders	Enabled

Contact Details

Commonwealth entities with questions regarding this advice should contact ASD Advice and Assistance by emailing asd.assist@defence.gov.au or by calling 1300 CYBER1 (1300 292 371).

Australian businesses or other private sector organisations seeking further information should contact CERT Australia by emailing info@cert.gov.au or by calling 1300 172 499.

[1] http://www.asd.gov.au/publications/protect/Application_Whitelisting.pdf
[2] http://www.asd.gov.au/publications/Top_4_Strategies_Explained.pdf
[3] http://technet.microsoft.com/en-us/library/hh831440.aspx
[4] http://technet.microsoft.com/en-us/library/ee844118.aspx
[5] http://www.asd.gov.au/publications/protect/Assessing_Security_Vulnerabilities_and_Patches.pdf
[6] http://www.microsoft.com/en-us/server-cloud/system-center/configuration-manager-2012.aspx
[7] http://technet.microsoft.com/en-us/windowsserver/bb332157.aspx
[8] http://www.asd.gov.au/publications/protect/Assessing_Security_Vulnerabilities_and_Patches.pdf
[9] http://technet.microsoft.com/en-us/windowsserver/bb332157.aspx
[10] http://www.asd.gov.au/publications/protect/Restricting_Admin_Privileges.pdf
[11] http://www.asd.gov.au/publications/Top_4_Strategies_Explained.pdf
[12] http://technet.microsoft.com/en-us/library/cc677002.aspx
[13] http://technet.microsoft.com/en-us/security/jj653751/
[14] http://technet.microsoft.com/en-us/security/jj653751
[15] http://technet.microsoft.com/en-us/sysinternals/bb896653
[16] http://technet.microsoft.com/en-us/sysinternals/bb545021.aspx
[17] http://technet.microsoft.com/en-us/security/jj653751
[18] http://technet.microsoft.com/en-us/security/jj653751
[19] http://support.microsoft.com/kb/243330
[20] http://www.asd.gov.au/publications/protect/Multi_Factor_Authentication.pdf
[21] http://support.microsoft.com/kb/2516445
[22] http://technet.microsoft.com/en-au/security/bulletin/MS13-063
[23] http://technet.microsoft.com/en-us/library/cc677002.aspx